Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

12 November 2015

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
richard.t.willis@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance (Base + Option):	7 February 2014 – 9 September 2016
Total Contract Amount (Base + Option):	$475,359 (Base) + $199,252 (Option)
Amount of Incremental Funds (Base + Option):	$440,469 (Base) + $115,189 (Option)
Total Amount Expended (thru 16 October – Base + Option):	$369,488 (Base) + $240 (Option)

Attention: Dr. Richard Willis
Subject: Quarterly Progress Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 NOV 2015		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **BBN Technologies,,10 Moulton Street,,Cambridge,,MA, 02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
In this report we summarize the technical progress accomplished during the third quarter of the second year of the SeaKey program. In this quarter we started work on our experimental option task and that progress will be reported here. This quarter we have continued work calculating the key rates achievable with different mode geometries capitalizing on multiple spatial modes to increase achievable key rates in high loss channels. In addition, we describe the initial designs for the CV-QKD transmitter and receiver we are planning to build, and provide an update on the ordering of equipment to build those sub-systems.

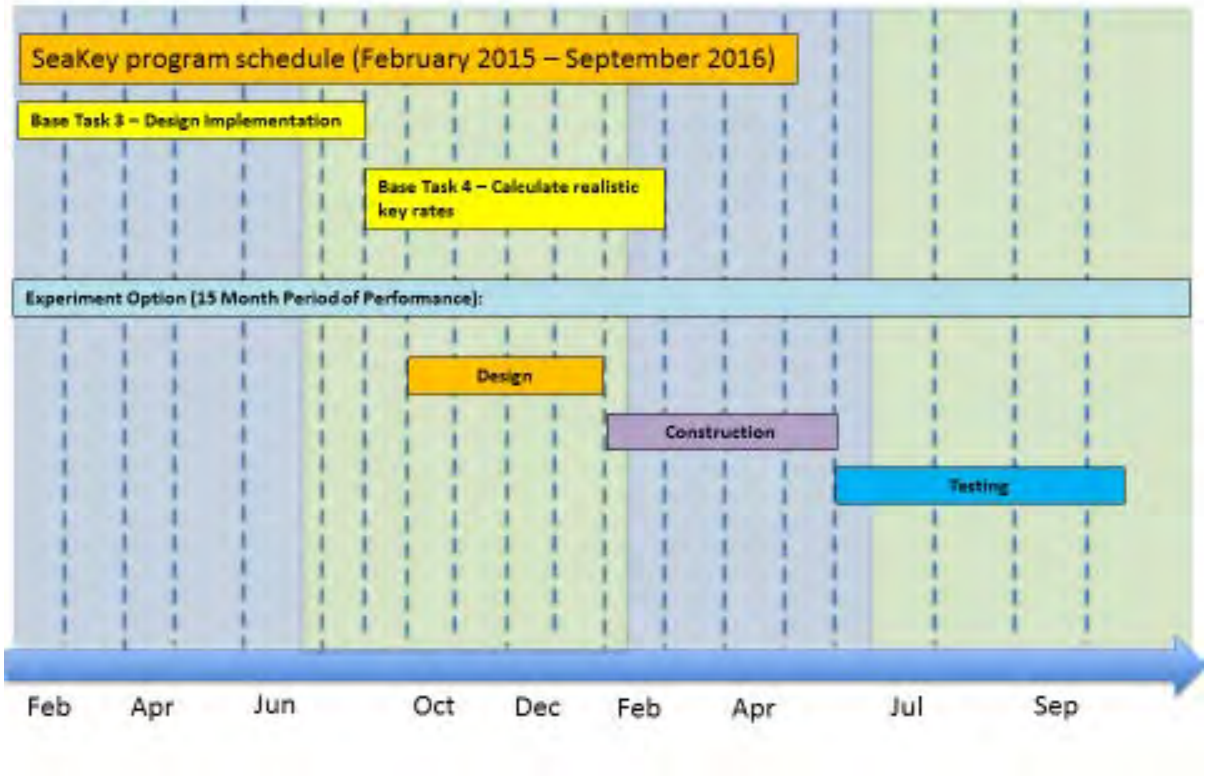
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**10**	

SEAKEY Quarterly Progress Report for the
Period 5 August 2015 – 13 November 2015 (100 Days)

Section A. Project Schedule

The Year 2 timeline below identifies the high level SeaKey tasks and approximate durations.



Section B. Technical Progress

SUMMARY

In this report we summarize the technical progress accomplished during the third quarter of the second year of the SeaKey program. In this quarter we started work on our experimental option task and that progress will be reported here.

This quarter we have continued work calculating the key rates achievable with different mode geometries capitalizing on multiple spatial modes to increase achievable key rates in high loss channels. In addition, we describe the initial designs for the CV-QKD transmitter and receiver we are planning to build, and provide an update on the ordering of equipment to build those sub-systems.

TECHNICAL RESULTS

Quantum key distribution using multiple Gaussian focused beams

As we stated in the previous report, recent proliferation of suggestions on using orbital angular momentum (OAM) modes for QKD applications begs a question of whether it is worth it (i.e., how much do we really gain after putting in the effort to generate and separate those orthogonal modes). Here is the list of some recent papers on this:

- http://iopscience.iop.org/1367-2630/17/3/033033/article
- http://www.nature.com/nphoton/journal/v9/n6/full/nphoton.2015.95.html
- http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.113.060503
- http://arxiv.org/pdf/1402.2602.pdf
- http://www.ncbi.nlm.nih.gov/pubmed/22714347
- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6671930
- http://cpl.iphy.ac.cn/fileup/PDF/201-1422.pdf

Laguerre-Gauss modes, which maintain their orthogonality when propagated through vacuum from one soft Gaussian aperture to another, also carry OAM. We have previously shown that OAM does not impact classical channel capacity (see http://www.opticsinfobase.org/abstract.cfm?URI=jon-4-8-501). The same restriction holds for the QKD rate, since it only depends on the loss and noise in the channel. However, the use of multiple, orthogonal spatial modes can improve QKD rate especially at short range (in the near-field regime), though the gain would almost certainly be offset by the losses in separation of the modes at the receiver. In fact, to the best of our knowledge, such separation has been achieved only for the azymuthal subset of LG modes, with considerable loss (see http://www.nature.com/ncomms/2013/131112/ncomms3781/full/ncomms3781.html and http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=1393220). We propose an alternative method of taking advantage of availability of multiple spatial modes in the near-field regime: using arrays of Gaussian focused beams at the receiver. While these beams are decidedly not orthogonal (they overlap), they do not require complex separation apparatus. Here we present our refined numerics demonstrating that they provide a substantial gain in QKD rate at close ranges that is comparable to what could be obtained if one had perfectly lossless separation of the azymuthal LG modes, and not far from the idealized scenario where one could use the entire orthogonal spatial mode set with soft Gaussian apertures.

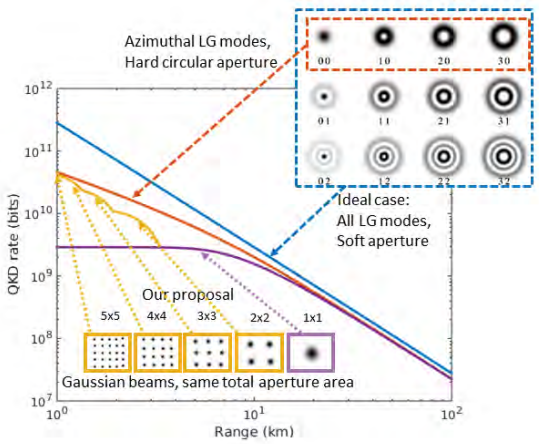


Figure 1 The comparison of the use of the multiple Gaussian laser beams vs. orthogonal modes.

Our recent calculations are in Figure 1. They are done a discrete-variable (decoy state) BB84 protocol and do not yet account for turbulence. The numerics have been refined since the last report. The purple curve is a single-spatial-mode baseline that uses one Gaussian laser beam for QKD. The yellow curve assumes multiple (an optimal number of) focused beams with an optimal choice of the nearest-neighbor overlap between spots at the receiver aperture plane (the optimal overlap is range dependent), and an optimal size of the beam waist. This calculation assumes a unity-fill factor single-photon detector array with each beam focused at the center of one detector pixel. The red curve uses azimuthal subset of LG modes propagated between hard circular apertures, where this subset of modes retains their orthogonality. Separation has been achieved for this subset of modes, however, here we assume that they are modulated and separated without loss (which is clearly being very optimistic). The blue curve uses orthogonal LG modes, assuming those spatial modes can be modulated and separated without loss (which is again being very optimistic). The blue curve assumes Gaussian (soft) apertures, the red curve assumes circular aperture of the same area as the soft aperture, and the other two curves (for the focused beam calculations) assume square apertures of the same area as the soft aperture.

The message from these results is:

1. One can gain a potentially between 1 to 2 orders of magnitude in key rate over a 1 km link by using multiple focused beams, BUT

2. Utilizing OAM modes for QKD is not worth it. The incremental gain by using the full set of LG modes is relatively small (at most a factor of 9, on average around factor of 7 in the near-field regime) and the losses associated with generating/separating these modes is likely to offset this gain.

3. Focused beams almost match the performance of the azimuthal subset of LG modes, which is the only set of OAM modes that have been separated in the laboratory.

In fact, the performance of the multiple focussed beam system (the red curve) might improve further if we use hexagonally-packed beam spots as opposed to using a square grid. However, we have not examined that yet.

We are currently working on the following:

1. further refining our numerics

2. extending these results to turbulent propagation (with and without adaptive optics). Turbulence will clearly adversely affect all the systems, but it is not clear which one (the multiple focused beam vs. the multiple LG modes) will be affected

Design for a Free-Space CV – QKD System

On the experimental option, we have begun to make progress on the design of the experimental implementation of a CV – QKD system for operation in free-space. Our first design – named 'Spiral 1' aims to design a traditional CV QKD system. The optical designs for the transmitter and receiver sub-systems for spiral 1 are shown in Figure 2 and Figure 3, respectively. The abbreviations for the optical components in the figures are as follows:

- VOA: variable optical attenuator
- Pol. Control: polarization controller
- A_mod: electro-optic amplitude modulator
- Φ_mod: electro-optic phase modulator

The transmitter shown in Figure 2 generates optical pulses by pulse carving from a CW laser source. The optical pulse is then split at a beamsplitter, toward an arm that encodes the CV state and an arm that prepares the local oscillator state, rotates its polarization with respect to the signal state and delays it with respect to the signal state. The polarization and temporal delay of the CV state relative to the signal state is aimed at making separation of those two states simpler at the receiver, mitigating the chance for noise from the LO to enter the signal channel. The CV encoded state and local

oscillator state are recombined at a second beamsplitter and transmitted into free-space through a fiber collimator.

At the receiver, shown in Figure 3, the signal from the transmitter is coupled into a fiber collimator, sent through polarization control and the CV state and the LO state are

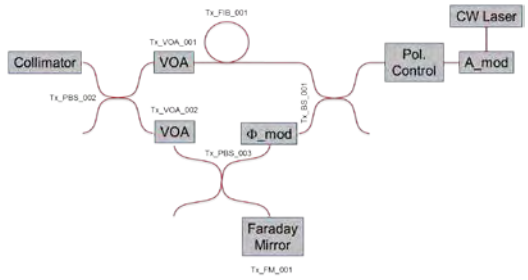


Figure 2 Transmitter design for CV QKD

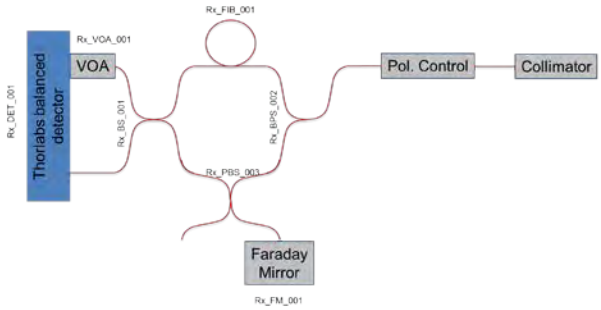


Figure 3 Receiver design for CV QKD

separated at a polarizing beam splitter. The CV state is delayed relative to the LO state, and the polarization of the LO state is again rotated using a Faraday mirror to match the CV state. The CV and LO are then mixed on a beamsplitter and detected in a balanced detector. One path of the optical beam leading to the balanced detector has a variable optical attenuator. This VOA is used to balance the optical intensity at the two ports of the balanced detector, mitigating common mode imbalances that could be attributed to beam-splitter or loss imperfections.

We have identified a number of risks associated with implementing this design. The two most critical risks are:

- The transmitter and receiver each have interferometers that need path length stability on the order of a fraction of a wavelength. This is achievable with passive stabilization – but that may not be practical in the fielded systems envisioned by the Navy. This is also achievable with active control systems, but that will increase the SWaP-C of the overall system.

- The LO needs to be transmitted through the channel – likely requiring several milliWatts of power at the receiver. Through a channel with appreciable loss, this would require many Watts of power at the transmitter, again increasing SWaP-C for the system.

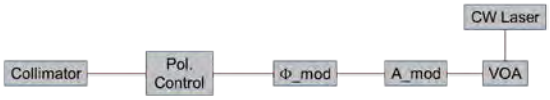


Figure 4 Spiral 2 transmitter design, following the self-referenced CVQKD proposal.

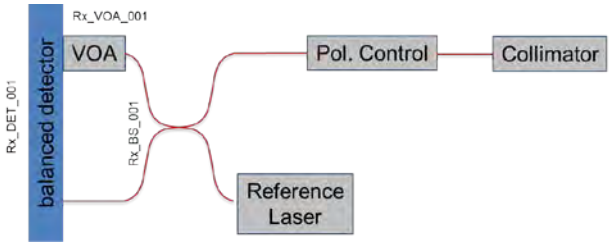


Figure 5 Spiral 2 receiver design, following the self-referenced CVQKD proposal.

Considering these risks we are currently evaluating a 'Spiral 2' design capitalizing on the latest proposal from Soh et. Al for a self-referenced Continuous Variable QKD protocol[1]. In this design, a local oscillator laser is located at the receiver to make coherent measurements on the CV state and the local oscillator state and compare the relative phase between the two signals to extract the measurements of the CV state phase and amplitude. We have made an initial spiral 2 design, shown in Figure 4 and Figure 5, which is drastically reduced in complexity and risk from that shown in Figure 2 and Figure 3.

Next Steps:

In the next quarter we will be receiving the parts to construct the designs shown in the optical diagrams above. We will be making laboratory measurements showing shot-noise limited performance of the receiver, and mapping the constellation of the 4 phase states required to implement the CV-QKD protocol. Finally, we will continue to work to identify a free-space path that we will use in future experiments to characterize CV-QKD in atmospheric conditions.

[1] Daniel B. S. Soh et. Al, "Self-referenced continuous-variable quantum key distribution protocol," arXiv:1503.04763v2.

Section C. Problem Areas – Identification

There are no problems or issues to report at this time.

Section D. Financial Update

Financial Charts reflecting Year 2: